

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-137686

(43)Date of publication of application : 31.05.1996

(51)Int.Cl.

G06F 9/06

G06F 12/14

(21)Application number : 07-237489

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 14.09.1995

(72)Inventor : YOSHIDA HIDEKI

IMAI TORU

SEGAWA HIDEO

(30)Priority

Priority number : 06221238

Priority date : 16.09.1994

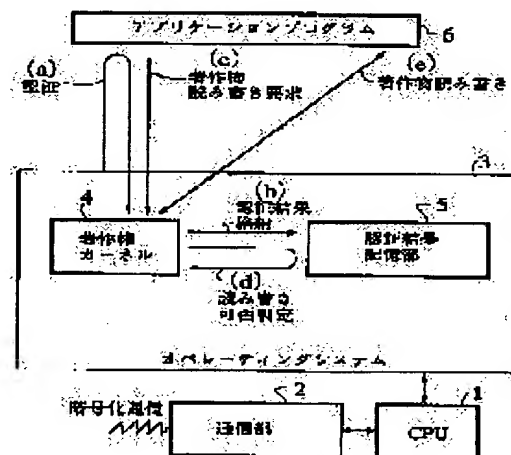
Priority country : JP

(54) METHOD AND DEVICE FOR MANAGING DATA ON LITERARY WORK

(57)Abstract:

PURPOSE: To prevent violation of copyright by verifying an application program and permitting an access request of the application program when the application program is verified when an access request is made from the application program to literary work data.

CONSTITUTION: A copyright kernel 4 in an operating system(OS) 3 executed by a CPU 1 verifies an application program 6 to discriminate whether or not the application program is a registered program. As a result of verification, when the application program is discriminated to be a program managing correctly a copyright label, it is stored in a storage section 5 in the OS. Then the usual application processing is executed and when the application program 6 makes a read/write request of literary work data to the OS, the OS 3 checks the storage section 5 and accepts the request when it is confirmed that the application program 6 manages the copyright label correct or rejects the request when not.



LEGAL STATUS

[Date of request for examination] 19.09.2000

[Date of sending the examiner's decision of rejection] 09.03.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

BEST AVAILABLE COPY

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision
of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

JP-A 8-137686

[0048]

(First Embodiment)

In the present embodiment, schematically, a copyright kernel and an authentication result storing mechanism are provided within the OS for performing authentication of the application program upon use of digital signatures.

[0051]

Thereafter, ordinary application processes are performed (S53 in Fig. 2), and in the event a read/write request of copyright data has been issued from the application program 6 to the OS (S54 in Fig. 2, c in Fig. 3), the OS 3 checks up in the above authentication result storing portion 5 (S55 in Fig. 2, d in Fig. 3), and when it is confirmed that the application program 6 properly manages the copyright label (a copyright-compliant application program), the request is accepted (S56 in Fig. 2, e in Fig. 3) but otherwise, rejects the request. With this arrangement, it is possible to perform proper copyright management.

<FIG. 2>

S51: Authenticate application
S52: Store authentication result
S53: Process application
S54: Request read/write of copyright
S55: Read/write availability judged?
S56: Read/write copyright

<FIG. 3>

- ① 6: Application program
- ②(a): Authentication
- ③(c) Request read/write of copyright
- ④(e): Read/write copyright
- ⑤ 4: Copyright kernel
- ⑥(b): Store authentication result
- ⑦ 5: Authentication result storing portion
- ⑧(d): Judge read/write availability
- ⑨ Operating System
- ⑩ Encoded communication
- ⑪ Communication portion

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-137686

(43)公開日 平成8年(1996)5月31日

(51)Int.Cl. ⁹	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 9/06	5 5 0 G	7230-5B		
12/14	3 1 0 A			

審査請求 未請求 請求項の数14 O L (全 18 頁)

(21)出願番号 特願平7-237489

(22)出願日 平成7年(1995)9月14日

(31)優先権主張番号 特願平6-221238

(32)優先日 平6(1994)9月16日

(33)優先権主張国 日本 (J P)

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 吉田 英樹

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72)発明者 今井 徹

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

(72)発明者 瀬川 英生

神奈川県川崎市幸区小向東芝町1 株式会
社東芝研究開発センター内

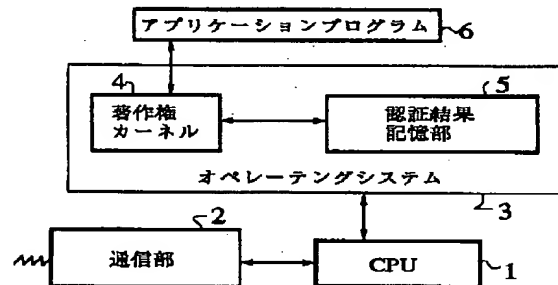
(74)代理人 弁理士 三好 秀和 (外3名)

(54)【発明の名称】 著作物データ管理方法及び著作物データ管理装置

(57)【要約】

【課題】 登録された正当なアプリケーションプログラムのみが絵画・小説などの受動的なデータである著作物を操作できるようにした著作物データ管理方法を提供すること。

【解決手段】 本発明は、マイクロプロセッサ上にて起動中の管理プログラムが、起動されたアプリケーションプログラムと所定の情報の受渡しを行うことによって、該アプリケーションプログラムの認証を行い、管理プログラムは、この認証の結果と、認証した前記アプリケーションプログラムを特定する情報とを組にして認証結果記憶手段に格納し、1つのアプリケーションプログラムから所望の著作物データへのアクセス要求が与えられた場合、管理プログラムは、認証結果記憶手段を参照し、該1つのアプリケーションプログラムが既に認証に成功したものであることが判明したときのみ該アクセス要求を許可することを特徴とする。



【特許請求の範囲】

【請求項 1】 アプリケーションプログラムを認証する認証手段と、

該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、

前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す時に要求された著作物データへのアクセスを許可する管理手段と、

を有することを特徴とする著作物データ管理装置。

【請求項 2】 前記アプリケーションプログラムは所定の暗号鍵で暗号化されており、前記認証手段は前記アプリケーションプログラムを前記所定の暗号鍵に対応する復号鍵で復号化することにより認証することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 3】 著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、正しいパスワードを記憶するパスワード記憶手段を更に有し、

前記認証手段は前記アプリケーションプログラムのパスワードを前記パスワード記憶手段に記憶された正しいパスワードと照合することにより前記アプリケーションプログラムを認証することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 4】 著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、複数のパスワードとそれらに対応する正しい応答を記憶するパスワード記憶手段を更に有し、

前記認証手段は前記アプリケーションプログラムに前記複数のパスワードの一つを通知し、前記アプリケーションプログラムから受けた応答を前記パスワード記憶手段に記憶された前記複数のパスワードの一つに対応する正しい応答と照合することにより前記アプリケーションプログラムを認証することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 5】 前記アプリケーションプログラムは第一のハードウェア内の第一のプロセッサ上で実行され、前記認証手段と前記記憶手段は第二のハードウェア内の第二プロセッサ上で動作し、前記管理手段は前記第一のハードウェア内の第一のプロセッサ上で動作し、前記第一のハードウェアと第二のハードウェアは互いに物理的に分離しており、前記第一のプロセッサと第二のプロセッサは互いに接続されていることを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 6】 前記認証手段は前記管理手段を含んだオペレーティングシステムが前記第一のプロセッサ上で起動された時に、該オペレーティングシステムも認証することを特徴とする請求項 5 記載の著作物データ管理装

置。

【請求項 7】 前記アプリケーションプログラムからのコールに応じて、著作物データの著作権ラベルに対する読み書き動作を行う著作物ラベル読み書きプログラムを更に有することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 8】 前記管理手段は、要求されたアクセスが著作物データの読み出しである時には、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示さない時にも要求された著作物データへのアクセスを許可することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 9】 前記管理手段は、どの著作物データがどのアプリケーションプログラムからアクセス可能であるかを示す情報を記憶し、前記管理手段は前記記憶手段に記憶された該情報に基づいて前記アプリケーションプログラムからの著作物データへのアクセス要求を許可することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 10】 前記認証手段は前記アプリケーションプログラムが起動された時に認証することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 11】 前記認証手段は前記アプリケーションプログラムが著作物データへのアクセス要求を発した時に認証することを特徴とする請求項 1 記載の著作物データ管理装置。

【請求項 12】 アプリケーションプログラムを認証する認証手段と、

該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、

前記アプリケーションプログラムから発行されるデータ入出力要求を、前記アプリケーションプログラムの識別子と共に受取る要求受理手段と、

前記要求受理手段で受取ったデータ入出力要求がデータ入力要求である時に要求されたデータを前記アプリケーションプログラムに入力するデータ入力手段と、

前記データ入力手段により入力されたデータが保護データであるかどうか判別する保護データ判別手段と、

前記保護データ判別手段が前記データ入力手段により入力されたデータを保護データであると判別した時に、少なくとも前記アプリケーションプログラムの識別子を記録する保護データ入力記憶手段と、

前記要求受理手段で受取ったデータ入出力要求がデータ出力要求である時に、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す場合及び前記アプリケーションプログラムの識別子が前記保護データ入力記憶手段に記録されていない場合にデータ出力を許可し、前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されている時にデータ出力を許可するか

どうかを少なくとも要求された出力先に基づいて判定する出力許可判定手段と、

前記出力許可判定手段がデータ出力を許可した時に要求されたデータを出力するデータ出力手段と、

を有することを特徴とする著作物データ管理装置。

【請求項 13】 アプリケーションプログラムを認証するステップと、該認証するステップにより得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶手段に記憶するステップと、

前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証するステップによる認証の成功を示す時に要求された著作物データへのアクセスを許可するステップと、
を有することを特徴とする著作物データ管理方法。

【請求項 14】 コンピュータに著作物データの管理を行わせるようにするためのコンピュータにより解読可能なコンピュータプログラムコード手段を実装したコンピュータで利用可能な媒体を有するコンピュータプログラム製品であって、該コンピュータプログラムコード手段が、コンピュータによって、アプリケーションプログラムを認証するようにする第一のコンピュータプログラムコード手段と、

コンピュータによって、該第一のコンピュータプログラムコード手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶するようにする第二のコンピュータプログラムコード手段と、

コンピュータによって、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記第二のコンピュータプログラムコード手段により記憶されている前記アプリケーションプログラムの認証結果が前記第一のコンピュータプログラムコード手段による認証の成功を示す時に要求された著作物データへのアクセスを許可するようにする第三のコンピュータプログラムコード手段とを有することを特徴とするコンピュータプログラム製品。

【発明の詳細な説明】

【0001】

【発明の属する技術】本発明は、計算機システム上で扱われる著作物データの管理を行う著作物データ管理方法および著作物データ管理装置に関する。

【0002】

【従来の技術】従来、計算機システム上にはセキュリティ機構があり、システム管理者が設定した権限にしたがってファイルなどのデータ管理が行なわれていた。計算機システムを所有する特定の組織および個人が閲覧・変更・配布などの操作を行なう権利を持つデータについては、このような管理が適切である。

【0003】ところが、プログラム・絵画・小説などの著作物を計算機システム上で扱う場合、システムを所有する組織および個人がその著作物の操作を行なう権利を持っていない場合が多い。具体的には、閲覧や利用はできても、変更や再配布が著作者によって認められていない場合などがある。

【0004】このような著作物を通常の計算機システムで扱う場合、悪意のシステム管理者がデータのアクセス権限を書き換えたり、システム管理者の権限でデータを読み書きすることによって、著作物を不当に利用されたりする危険がある。

【0005】このような不都合を回避するため、プログラムの利用の可否をシステム管理者にも侵害できないような方法で管理する「超流通」という概念が提唱されている（森亮一、田代秀一「ソフトウェア・サービス・システム（SSS）の提案」電子情報通信学会論文誌 '87/1 Vol. J70-D No.1 参照）。超流通システムでは、著作物に著作者・利用／配布条件・課金方法などを示すラベル（著作権ラベル）がついており、そのラベルは通常のソフトウェアでは変更することができない。これによって、アプリケーションプログラムの著作権保護を行なうことはできる。

【0006】これとは別に、米国防総省のOS（オペレーティングシステム）のセキュリティレベル分類（Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense Standard DOD 5200.28-STD, Library Number S225,711, December 1985, 通称 Orange Book）でセキュリティレベルBに分類されるようなOSでは、強制保護という機構を用いることによって、あるデータを読み書きすることを許されているプログラムまたはユーザが、そのデータを、そのデータを読み書きすることを許されていないプログラムまたはユーザに渡すことができないようにすることができる。この方法を著作物に応用することによって、プログラムコードを持たないデータを含めたファイルの保護を行なうこともできる。

【0007】しかしながら、上記のような従来の著作権管理機構では著作権保護を行なう対象はプログラムのみであり、絵画・小説などプログラムコードを持たずに他のプログラムに読み込まれて利用される受動的なデータである著作物を保護する機構は提供されていない。

【0008】例えば、受動的な著作物に著作権ラベルをつけて保護しようとしても、著作物を読んだ悪意のアプリケーションプログラムが著作権ラベルを不正に管理することが可能である。著作権ラベルの不正な管理方法としては、著作権ラベルを改ざんまたは除去して著作物をコピーするという可能性が挙げられる。

【0009】また、一部の著作物は、他の著作物の中を含むような形で作成されている場合がある。たとえば、あるテーマに基づいて複数の絵画の画像を編集して画集

を作るといった場合、画集（二次著作物）の著作権のほかに、元の個々の絵画（一次著作物）の著作権をも管理する必要がある。従って、複数の絵画データを編集して画集を作成する機能を持つアプリケーションプログラムでは、一次著作物につけられた著作権ラベルの中の著作者・利用／配布条件・課金方法などを損なわないような著作権ラベルを二次著作物に付加しなければならない。具体的には、著作者として一次著作物の著作者をすべて含め、すべての著作者の利用／配布条件で許されているような利用／配布方法のみを許すほか、すべての著作者にそれぞれ課金が行なわれるような著作権ラベルをつけるといった機構が必要である。

【0010】ところが、従来の著作管理機構では、アプリケーションプログラムがこのように著作権ラベルを管理することが保証されない。そのため、従来の機構で著作物を保護しようとする、例えば著作権をアプリケーションプログラムの中にあらかじめ埋め込んでおく必要がある。しかしながら、この方式には、処理の自由度や処理速度が低下する問題がある。さらに、データを読み込んで操作するように書かれた既存のアプリケーションプログラムを修正して著作権管理を行なうように利用することは困難であり、新たにアプリケーションプログラムを開発する必要があるという不具合がある。

【0011】従来の著作物を保護する方法としては、上記のほかに、著作物を直接アプリケーションプログラムに読み込ませず、毎回OSを経由して著作物に対する操作を行なわせるという方法がある。しかしながら、この方法では、OSが対応した処理しか行なえないため、アプリケーションプログラムに特有な処理を行なうことができないほか、処理のたびにOSが呼び出されるために実行時間がかかるという問題がある。

【0012】一方、従来のセキュリティレベルBのOSでは、アプリケーションプログラムにあるデータが渡されると、そのアプリケーションプログラムがそのデータを読んだ以降にデータを書き込むファイルすべてに、そのデータに基づいて作られたデータが書き込まれる可能性がある、という前提でOSによる管理が行なわれる。

【0013】このようなOSを使って著作物管理を行なうと、複数の著作物を次々に読み書きしたりするようなアプリケーションプログラムでは、それまでに一度でも読み込んだ著作物の著作権ラベルが、それ以降に書き込まれた著作物ファイルすべてに付加されるため、本来無関係な著作権ラベルが著作物につけられてしまう場合がある、という問題点がある。

【0014】

【発明が解決しようとする課題】従来の著作物に著作権ラベルを付加するような著作管理機構では著作権保護を行なう対象はプログラムのみであり、絵画・小説などプログラムコードを持たずに他のプログラムに読み込まれて利用される受動的なデータである著作物を保護する機

構は提供されていなかった。

【0015】また、従来のOSを使って著作物管理を行なうような著作管理機構では、絵画・小説などの受動的なデータである著作物に対するアクセスを伴う処理のたびにOSが呼び出されるため、処理の実行に時間がかかるという問題点、あるいは著作権ラベルのきめ細かい管理ができず、それまでに一度でも読み込んだ著作物の著作権ラベルが、それ以降に書き込まれた著作物ファイルすべてに付加される問題点などがあつた。

【0016】本発明は、上記事情を考慮してなされたものであり、絵画・小説などプログラム以外の受動的なデータである著作物に対しても、著作権ラベルの管理を正しく行なうものとして登録されたアプリケーションプログラムのみが操作できるような管理のできる著作物データ管理方法及び著作物データ管理装置を提供することを目的とする。

【0017】

【課題を解決するための手段】本発明は、アプリケーションプログラムを認証する認証手段と、該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す時に要求された著作物データへのアクセスを許可する管理手段と、を有する著作物データ管理装置を提供する。

【0018】又、本発明は、前記アプリケーションプログラムは所定の暗号鍵で暗号化されており、前記認証手段は前記アプリケーションプログラムを前記所定の暗号鍵に対応する復号鍵で復号化することにより認証することを特徴とする。

【0019】又、本発明は、著作物データに対するアクセスが許可されるべき各著作権遵守アプリケーションプログラムについて、正しいパスワードを記憶するパスワード記憶手段を更に有し、前記認証手段は前記アプリケーションプログラムのパスワードを前記パスワード記憶手段に記憶された正しいパスワードと照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【0020】又、本発明は、著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、複数のパスワードとそれらに対応する正しい応答を記憶するパスワード記憶手段を更に有し、前記認証手段は前記アプリケーションプログラムに前記複数のパスワードの一つを通知し、前記アプリケーションプログラムから受けた応答を前記パスワード記憶手段に記憶された前記複数のパスワードの一つに対応する正しい応答と照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【0021】又、本発明は、前記アプリケーションプログラムは第一のハードウェア内の第一のプロセッサ上で実行され、前記認証手段と前記記憶手段は第二のハードウェア内の第二プロセッサ上で動作し、前記管理手段は前記第一のハードウェア内の第一のプロセッサ上で動作し、前記第一のハードウェアと第二のハードウェアは互いに物理的に分離しており、前記第一のプロセッサと第二のプロセッサは互いに接続されていることを特徴とする。

【0022】又、本発明は、前記認証手段は前記管理手段を含んだオペレーティングシステムが前記第一のプロセッサ上で起動された時に、該オペレーティングシステムも認証することを特徴とする。

【0023】又、本発明は、前記アプリケーションプログラムからのコールに応じて、著作物データの著作権ラベルに対する読み書き動作を行う著作物ラベル読み書きプログラムを更に有することを特徴とする。

【0024】又、本発明は、前記管理手段は、要求されたアクセスが著作物データの読み出しである時には、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示さない時にも要求された著作物データへのアクセスを許可することを特徴とする。

【0025】又、本発明は、前記管理手段は、どの著作物データがどのアプリケーションプログラムからアクセス可能であるかを示す情報を記憶し、前記管理手段は前記記憶手段に記憶された該情報に基づいて前記アプリケーションプログラムからの著作物データへのアクセス要求を許可することを特徴とする。

【0026】又、本発明は、前記認証手段は前記アプリケーションプログラムが起動された時に認証することを特徴とする。

【0027】又、本発明は、前記認証手段は前記アプリケーションプログラムが著作物データへのアクセス要求を発した時に認証することを特徴とする。

【0028】更に、本発明は、アプリケーションプログラムを認証する認証手段と、該認証手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶する記憶手段と、前記アプリケーションプログラムから発行されるデータ入出力要求を、前記アプリケーションプログラムの識別子と共に受取る要求受理手段と、前記要求受理手段で受取ったデータ入出力要求がデータ入力要求である時に要求されたデータを前記アプリケーションプログラムに入力するデータ入力手段と、前記データ入力手段により入力されたデータが保護データであるかどうか判別する保護データ判別手段と、前記保護データ判別手段が前記データ入力手段により入力されたデータを保護データであると判別した時に、少なくとも前記アプリケーションプログラムの識別子を記録する保護データ入力記

憶手段と、前記要求受理手段で受取ったデータ入出力要求がデータ出力要求である時に、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証手段による認証の成功を示す場合及び前記アプリケーションプログラムの識別子が前記保護データ入力記憶手段に記録されていない場合にデータ出力を許可し、前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されている時にデータ出力を許可するかどうかを少なくとも要求された出力先に基づいて判定する出力許可判定手段と、前記出力許可判定手段がデータ出力を許可した時に要求されたデータを出力するデータ出力手段と、を有する著作物データ管理装置を提供する。

【0029】更に、本発明は、アプリケーションプログラムを認証するステップと、該認証するステップにより得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶手段に記憶するステップと、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証するステップによる認証の成功を示す時に要求された著作物データへのアクセスを許可するステップと、を有する著作物データ管理方法を提供する。

【0030】又、本発明は、前記アプリケーションプログラムは所定の暗号鍵で暗号化されており、前記認証するステップは前記アプリケーションプログラムを前記所定の暗号鍵に対応する復号鍵で復号化することにより認証することを特徴とする。

【0031】又、本発明は、著作物データに対するアクセスが許可されるべき各著作権遵守アプリケーションプログラムについて、正しいパスワードをパスワード記憶手段に記憶するステップを更に有し、前記認証するステップは前記アプリケーションプログラムのパスワードを前記パスワード記憶手段に記憶された正しいパスワードと照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【0032】又、本発明は、著作物データに対するアクセスが許可されるべき著作権遵守アプリケーションプログラムについて、複数のパスワードとそれらに対応する正しい応答をパスワード記憶手段に記憶するステップを更に有し、前記認証するステップは前記アプリケーションプログラムに前記複数のパスワードの一つを通知し、前記アプリケーションプログラムから受けた応答を前記パスワード記憶手段に記憶された前記複数のパスワードの一つに対応する正しい応答と照合することにより前記アプリケーションプログラムを認証することを特徴とする。

【0033】又、本発明は、前記アプリケーションプログラムは第一のハードウェア内の第一のプロセッサ上で

実行され、前記認証するステップと前記記憶するステップは第二のハードウェア内の第二プロセッサ上で行われ、前記許可するステップは前記第一のハードウェア内の第一のプロセッサ上で行われ、前記第一のハードウェアと第二のハードウェアは互いに物理的に分離しており、前記第一のプロセッサと第二のプロセッサは互いに接続されていることを特徴とする。

【0034】又、本発明は、前記認証するステップは前記許可するステップを行うオペレーティングシステムが前記第一のプログラム上で起動された時に、該オペレーティングシステムも認証することを特徴とする。

【0035】又、本発明は、前記アプリケーションプログラムから著作物ラベル読み書きプログラムをコールするステップと、著作物データの著作権ラベルに対する読み書き動作を前記著作権ラベル読み書きプログラムにより行うステップと、を更に有することを特徴とする。

【0036】又、本発明は、前記許可するステップは、要求されたアクセスが著作物データの読み出しである時には、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記するステップによる認証の成功を示さない時にも要求された著作物データへのアクセスを許可することを特徴とする。

【0037】又、本発明は、前記記憶手段は、どの著作物データがどのアプリケーションプログラムからアクセス可能であるかを示す情報を記憶し、前記許可するステップは前記記憶手段に記憶された該情報に基づいて前記アプリケーションプログラムからの著作物データへのアクセス要求を許可することを特徴とする。

【0038】又、本発明は、前記認証するステップは前記アプリケーションプログラムが起動された時に認証することを特徴とする。

【0039】又、本発明は、前記認証するステップは前記アプリケーションプログラムが著作物データへのアクセス要求を発した時に認証することを特徴とする。

【0040】更に、本発明は、アプリケーションプログラムを認証するステップと、該認証するステップにより得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶手段に記憶するステップと、前記アプリケーションプログラムに保護データが入力された時に、少なくとも前記アプリケーションプログラムの識別子を保護データ入力記録手段に記録するステップと、前記アプリケーションプログラムからのデータ出力要求に対し、前記記憶手段に記憶されている前記アプリケーションプログラムの認証結果が前記認証するステップによる認証の成功を示す場合及び前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されていない時にデータ出力を許可し、前記アプリケーションプログラムの識別子が前記保護データ入力記録手段に記録されている時にデータ出力を許可するかどうかを少なくとも要求され

た出力先に基づいて判定するステップと、を有する著作物データ管理方法を提供する。

【0041】更に、本発明は、コンピュータに著作物データの管理を行わせるようにするためのコンピュータにより解読可能なコンピュータプログラムコード手段を実装したコンピュータで利用可能な媒体を有するコンピュータプログラム製品であって、該コンピュータプログラム手段が、コンピュータによって、アプリケーションプログラムを認証するようにする第一のコンピュータプログラムコード手段と、コンピュータによって、該第一のコンピュータプログラムコード手段により得られた該アプリケーションプログラムの認証結果を該アプリケーションプログラムの識別子と対応させて記憶するようにする第二のコンピュータプログラムコード手段と、コンピュータによって、前記アプリケーションプログラムからの著作物データへのアクセス要求を受け、前記第二のコンピュータプログラムコード手段により記憶されている前記アプリケーションプログラムの認証結果が前記第一のコンピュータプログラムコード手段による認証の成功を示す時に要求された著作物データへのアクセスを許可するようにする第三のコンピュータプログラムコード手段とを有することを特徴とするコンピュータプログラム製品を提供する。

【0042】本発明では、著作権ラベルを正しく管理すること、つまり、著作権ラベルを除去・改ざんしたりしないほか、一次著作物の著作権ラベルを反映した著作権ラベルを二次著作物に付加する、ということを著作物を扱うアプリケーションプログラムが遵守するものとする。これは、著作物と著作物を扱うアプリケーションプログラムの作成者が同一ならば実現可能であるほか、作成者が同一でなくても、アプリケーションプログラムを管理機関に登録することにしてもよい。上記の条件を満たすアプリケーションプログラムを著作権遵守アプリケーションプログラムと呼ぶ。

【0043】実行時には、アプリケーションプログラムが著作権遵守アプリケーションプログラムであるかどうかを認証する。例えば、OSで管理されるファイルなどのデータには、そのデータが著作物であるかどうかを判断するための情報が付加される。

【0044】著作権遵守アプリケーションプログラムであることが認証されたアプリケーションプログラムには、著作権データを直接読むことを許すほか、著作物データを作成する（データに著作権ラベルをつける）ことも許す。著作権遵守アプリケーションプログラム以外のアプリケーションプログラムには、著作物データを直接読み書きすることを許さない。

【0045】さらに、本発明では、著作権遵守アプリケーションプログラムを実行させるプロセッサと、認証や認証結果を格納させるプロセッサとを、互いに異なるものとする。これによってさらに、認証や著作権データ管

理など著作物管理に関わらない前者のプロセッサに係わる部分の管理だけを利用者が行なえるようにし、一方、システム管理者の権限で著作権データ等を不正に管理するなどができないようにすることが可能となる。よって、極めて高いセキュリティを実現できる。また、本体のOSおよびアプリケーションプログラムへの侵入が生じた場合でも、別プロセッサに係わる認証結果が改ざんされにくいいため、著作権の侵害をより効果的に防止することができる。

【0046】このように本発明によれば、著作権ラベルの管理を正しく行なうアプリケーションプログラムのみが著作物を操作でき、それ以外のアプリケーションプログラムからの著作物の操作を禁止できるため、著作権の侵害の危険なしに計算機システム上で著作物を処理することができる。

【0047】

【発明の実施の形態】以下、図面を参照しながら本発明の実施の形態を説明する。

【0048】（第1の実施の形態）本実施の形態は、概略的には、著作権カーネルと認証結果記憶機構をOS内に設け、デジタル署名を用いてアプリケーションプログラムの認証を行なうものである。

【0049】図1に、本実施の形態の概略的なシステム構成図を示す。本実施の形態では、アプリケーションプログラム6のベンダは、アプリケーションプログラム6が著作権ラベルを正しく管理することを保証するものとする。すなわち、アプリケーションプログラム6は、著作権ラベルを除去・改ざんしたりしないほか、一次著作物の著作権ラベルを反映した著作権ラベルを二次著作物に付加する、ということを著作物を扱うアプリケーションプログラムが遵守するものとする。これは、著作物と著作物を扱うアプリケーションプログラムの作成者が同一ならば実現可能であるほか、作成者が同一でなくても、アプリケーションプログラムを管理機関に登録することにしてもよい。上記の条件を満たすアプリケーションプログラムを、「著作権遵守アプリケーションプログラム」と呼ぶ。

【0050】以下、本実施の形態の動作を図2のフローチャートと図3の動作説明図に基づいて説明する。まず、CPU1上で実行されるオペレーティングシステム(OS)3内の著作権カーネル4は、アプリケーションプログラム6を認証し、アプリケーションプログラムが登録されたものであるかを判定する(図2のS51、図3中のa)。認証の結果、著作権ラベルを正しく管理するアプリケーションプログラムであることが判明した場合は、OS内にある認証結果記憶部5中にその旨を記憶しておく(図2のS52、図3中のb)。

【0051】その後、通常のアプリケーションの処理が行なわれ(図2のS53)、アプリケーションプログラム6から著作物データの読み書き要求がOSに対して発

せられた際には(図2のS54、図3中のc)、OS3は上記の認証結果記憶部5中を調べ(図2のS55、図3中のd)、アプリケーションプログラム6が著作権ラベルを正しく管理するもの(著作権遵守アプリケーションプログラム)であることが確認されたときはその要求を認めるが(図2のS56、図3中のe)、そうでなければ要求を拒否する。これによって、著作物管理を正しく行なうことができる。

【0052】本システムは、外部と通信装置2(例えばモデム、LANアダプタカード、SCSIインタフェースカードなど)によって接続され、図示しないネットワーク経由にて外部との間で著作物データをやり取りすることができる。ネットワーク上の著作物データは、暗号化などの手段を利用することによって保護することが可能である。

【0053】本実施の形態では、OS3の管理は、著作物管理を行なう組織の管理者が行ない、このシステムを利用する組織または個人(以下「利用者」)に対してシステム管理を行なう機能は提供しないものとする。このため、著作権カーネル4や認証結果記憶部5を改ざんすることはできないので、著作物は正しく管理される。

【0054】さて、本実施の形態では認証の方法として、公開鍵暗号方式を用いたアプリケーションプログラムの実行ファイルへのデジタル署名を用いることができる。

【0055】図4は、本実施の形態の認証を行なう部分の概略構成図である。アプリケーションプログラム6のベンダは、アプリケーションプログラム6が著作権ラベルを正しく管理することを確認した後、非公開の暗号化鍵を用いてアプリケーションプログラム6を暗号化する。利用者には、この暗号化されたファイルを配布する。アプリケーションプログラム6を復号化するための復号化鍵は、公開しておく。あるいは、復号化鍵は、アプリケーションの使用を許可されている使用者に対してのみあらかじめ渡しておくようにしても良い。

【0056】OS3内には、著作権カーネル4と呼ばれる部分があり、ここで著作権に関連する処理を行なう。以下、著作権カーネル4での具体的な処理について述べる。

【0057】アプリケーションプログラム6の実行時には、著作権カーネル4が、暗号化された(アプリケーションプログラム6Aの)ファイルを公開鍵によって復号化する(図4中のa)。復号が成功すれば、それはアプリケーションプログラム6が正しく認証されたことになるので、得られた平文の実行ファイル(アプリケーションプログラム6B)を実行するとともに、認証結果記憶部5に認証が成功した旨を記憶する(図4中のb)。

【0058】図5は、図4の認証結果記憶部5内に設けられた管理テーブルの構造を示す図である。各アプリケーションプログラムごとに、そのアプリケーションプロ

グラムが著作権遵守アプリケーションプログラムであるかどうか記憶されている。

【0059】この実施の形態によれば、著作権遵守アプリケーションプログラムと、利用者が独自に作成したそれ以外のアプリケーションプログラムとを区別することができる。また、利用者が、著作権遵守アプリケーションプログラムをリバースエンジニアリングによって解析した上で改ざんして著作権ラベルを不正に操作するように改造しようとしても、著作権遵守アプリケーションプログラムが非公開鍵によって暗号化されているため、一般利用者には正しく暗号化を行なうことができず、復号化の際に正しく復号化されないことによって改ざんが発覚する。

【0060】このように本実施の形態によれば、デジタル署名を用いた認証によって著作権遵守アプリケーションプログラムが判別でき、アプリケーションプログラムが著作権ラベルを不正に操作することによる著作権の侵害を防止できる。また、利用者がアプリケーションプログラムを解析して変更することはできないので、高いセキュリティを実現することができる。

【0061】ここで、著作権の侵害の可能性については、認証されたアプリケーションプログラムは著作権ラベルの管理を正しく行なうことをアプリケーションプログラム作成者が保証しているため、これらのアプリケーションプログラムが著作権を侵害することはない。また、認証されていないアプリケーションプログラムが著作物データを読み書きすることを禁じることができるため、これらのアプリケーションプログラムによって著作権が侵害されることもない。

【0062】著作権遵守アプリケーションプログラムのみが著作物を読んだり一次著作物からの二次著作物の作成を行ったりすることができるため、アプリケーションプログラムが渡された著作物データを自由に処理することができる。また、アプリケーションプログラムにデータを直接渡さないシステムと比べ、既存のアプリケーションプログラムにわずかな改造を加えるだけで著作権ラベルを正しく扱うアプリケーションプログラムにすることが可能である。またその際、著作物の処理を行う場合にOSを毎回呼び出す必要がないため、実行速度の向上を図ることができる。

【0063】また、一次著作物の二次著作物での（二次利用）の細かい管理が可能になるという利点もある。一般に、一次著作物のどの部分がどの二次著作物に二次利用されているかという情報は、アプリケーションプログラムでの処理の詳細を把握していないOSで管理することは困難である。このような二次利用関係はアプリケーションプログラムがもっとも正確に把握している。

【0064】本実施の形態では、アプリケーションプログラムが著作物データを生成することを許すため、アプリケーションプログラムが二次著作物の著作権ラベルを

生成することができる。このため、一次著作物の著作権を二次著作物に正確に反映することができる。

【0065】次に、上記第1の実施の形態に対する変形例1～変形例9を説明する。

（変形例1）認証の方法として、第1の実施の形態のデジタル署名の代わりにパスワードを用いることができる。

【0066】図6は、変形例1の認証を行なう部分の概略構成図である。この他の部分は第1の実施の形態（図1）と同様であるので省略する。

【0067】本変形例1では、アプリケーションプログラム6はパスワードを持っており、アプリケーションプログラム6の実行時にOS3に対して自分が持っているパスワードを提示する（図6中のa）。著作権カーネル4はアプリケーションプログラム6のIDとパスワードをパスワード記憶部15中に格納された各著作権遵守アプリケーションプログラムのIDおよび全ての著作権遵守アプリケーションプログラムに共通なパスワードと照合し（図6中のb）、正しいパスワードが提示された場合にのみ、認証結果記憶部5に認証が成功した旨を記憶する（図6中のc）。

【0068】本変形例1は、暗号化が不要であることから、第1の実施の形態に比較して、アプリケーションプログラムの起動がより高速であるとともに、装置構成が簡略化されるという利点がある。

【0069】（変形例2）図7は、変形例2の認証を行なう部分の概略構成図である。この他の部分は第1の実施の形態（図1）と同様であるので省略する。

【0070】変形例1では、パスワードが固定されていると、そのパスワードが漏洩した場合に認証が正しく行なわれない場合がある。この変形例2では、全ての著作権遵守アプリケーションプログラムに共通なパスワードを一つではなく複数用意しておく。具体的には、合言葉を取り決めておき、OS3側がまず取り決めておいた単語（数値などを含む）を一つ選んでアプリケーションプログラム6に通知する（図7中のa）。アプリケーションプログラム6は、その合言葉に対してあらかじめ決められた返答を返す（図7中のb）。著作権カーネル4は、その返答をパスワード記憶部15内の返答と照合し（図7中のc）、正しい返答を答えた場合のみ、認証結果記憶部5に認証が成功した旨を記憶する（図7中のd）。

【0071】本変形例2は、パスワードの漏洩によってアプリケーションプログラム6が正しく認証できなくなる危険が変形例1より小さい利点がある。

【0072】（変形例3）本変形例3は、システムから著作物管理を行なう部分とそうでない部分を互いに分離し、それらを異なるハードウェア上で実現することによって、著作物管理に関わらない部分の管理だけをユーザーが行なえるようにし、一方、システム管理者の権限で著

著作権ラベルを不正に管理することができないようにして、極めて高いセキュリティを実現できるようにしたものである。これによって、UNIXなどの従来のOSをベースにしてシステムを構成することができる。

【0073】図8に、本変形例の概略的なシステム構成図を示す。著作物管理を行なう著作権カーネル4と認証結果記憶部5とを本体OS14から分離し、それらを別のCPU21上に搭載し、本体ハードウェア30のCPU11と別ハードウェア32の別CPU21との間をバス12によって結合する。

【0074】本変形例3の処理の手順は、第1の実施の形態と同様である。まず、アプリケーションプログラム6のベンダは、アプリケーションプログラム6が著作権ラベルを正しく管理することを保証するものとする。このような保証が行なわれたアプリケーションプログラム6は、あらかじめ著作物管理を行なう組織に登録される。

【0075】別CPU21上にて提供される著作権カーネル4は、アプリケーションプログラム6を認証し、アプリケーションプログラムが登録されたものであるかを判定する(図8中のa)。認証の結果、著作権ラベルを正しく管理するアプリケーションプログラムであることが判明した場合は、認証結果記憶部5中にその旨を記憶しておく(図8中のb)。

【0076】その後、アプリケーションプログラム6から著作物データの読み書き要求が本体OS14に対して発せられた際には(図8中のc)、本体OS14は上記の認証結果記憶部5中を調べ(図8中のd)、アプリケーションプログラム6が著作権ラベルを正しく管理するもの(著作権遵守アプリケーションプログラム)であることが確認されたときはその要求を認めるが(図8中のe)、そうでなければ要求を拒否する。

【0077】これによって、悪意の管理者が本体ハードウェア30側の本体OS14の設定を書き換えて著作物データを改ざんしようとしても、著作物データを管理する著作権カーネル4および認証結果記憶部5はハードウェア的に分離されているため、改ざんすることはできない。したがって、本体ハードウェア30を利用者に管理させても著作物を正しく管理することができる。

【0078】(変形例4)アプリケーションプログラム6の認証が正しく行なわれても、本体OS14が改ざんされると、著作物の読み書き可否判定を正しく行なわれないようにしたり、著作物データを正しく管理できないようにされたりする危険がある。

【0079】これを防ぐため、変形例3を修正し、計算機システムの起動時に本体OS14の認証を行なうようにしたのが本変形例である。

【0080】本変形例4の概略構成図を、図9に示す。計算機システムの起動時には、まず別CPU21が起動され(図9中のa)、その後本体CPU11上の本体

OS14が起動する際(図9中のc)に、別CPU21上のプログラムによって本体CPU11上の本体OS14が認証される(図9中のb)。

【0081】別CPU21による本体ハードウェア30側の本体OS14の認証方法としては、前述したOSによるアプリケーションプログラムの認証と同様の方法が利用できる。

【0082】(変形例5)第1の実施の形態では、各アプリケーションプログラムで個別に著作権ラベルの読み書きをする。この操作を一つのプログラムにまとめたものを著作権ラベル読み書きプログラムとし、このプログラムを著作権遵守アプリケーションプログラムが呼び出して、著作権ラベルの読み書きをさせるようにすることもできる。

【0083】本変形例5の概略構成図を、図10に示す。各アプリケーションプログラム61〜63々は、著作権ラベル読み書きプログラム64を呼び出し(図10中のa)、呼び出された著作権ラベル読み書きプログラム64が、実際の著作権ラベル160の読み書きを行なう(図10中のb)。

【0084】この変形例によると、アプリケーションプログラムごとに著作権ラベルの読み書き処理を行なうルーチンを作らずに済み、開発効率上がるほか、アプリケーションプログラムがライブラリ、即ち著作権ラベル読み書きプログラム、を正しく利用するかぎり、著作権ラベルに対して誤った管理が行なわれる可能性がなくなる。

【0085】(変形例6)第1の実施の形態においては、認証されていないアプリケーションプログラムについては、著作物データの読み書き両方を禁止していたが、本変形例6は、書き込みのみを禁止し、読み出しは認証されていないアプリケーションプログラムについても許す。

【0086】このようにしても、アプリケーションプログラムが著作物を他へコピーすることができないので、著作権侵害を防止するという目的を達成することができる。

【0087】(変形例7)第1の実施の形態では、アプリケーションプログラムは著作権遵守アプリケーションプログラムであるかそうでないかの二通りに分類し、唯一の機関がアプリケーションプログラムの管理を行い、著作物を操作するすべてのアプリケーションプログラムはその機関に登録するものであった。

【0088】本変形例では、上記の分類を細分化し、「各著作物のベンダがどのアプリケーションプログラムを信頼するか」を自由に決定することができるようにする。これによって、集中管理を行なう管理機関が不要となる利点がある。

【0089】また、各著作物を作成するベンダが、信頼できるベンダ、つまり自社・関連会社・契約を行なった

10

20

30

40

50

会社などが作成したアプリケーションプログラムからの読み書きのみを個別に許すことができるため、著作権の保護をよりきめ細かく行なうことができる。

【0090】図11が、本変形例における認証結果記憶部5内に設けられた管理テーブルの構造を示す図である。各アプリケーションプログラムごとに、そのアプリケーションプログラムがどの著作物を読み書きすることが許されているか、が記憶されている。即ち、各アプリケーションプログラムが各著作物について認証されたかどうか記憶されている。

【0091】本変形例では、認証として、第1の実施の形態または変形例1、2と同じ方法を用いれば良い。

【0092】本変形例によれば、万一著作物ラベルを正しく管理しないアプリケーションプログラムが登録されても、広い範囲で著作権侵害が生じることを防止することができる。

【0093】(変形例8) 第一の実施の形態では、認証を予め行っているが、これを変形して、アプリケーションプログラムが著作物の読み書き要求を行ったときにはじめて認証を行うようにすることも可能である。この場合、システム構成は上述した図1に示すものと同様である。

【0094】以下、図12に示すフローチャートに従って、本変形例における動作手順を説明する。

【0095】まず、CPU1上で実行されるアプリケーションプログラム6の通常の処理が行われ(図12のS61)、アプリケーションプログラム6からOS3に対して著作物の読み書き要求が発せられた場合(図12のS62)、OS3は内部の認証結果記憶部5を調べて、アプリケーションプログラム6の認証が既に行われているかどうか確かめる(図12のS63)。

【0096】また認証が行われておらず、認証結果記憶部5にアプリケーションプログラム6の認証結果が記録されていない場合には、OS3内の著作権カーネル4がアプリケーションプログラム6を認証し、このアプリケーションプログラムが登録されたものであるかどうか判定する(図12のS64)。この認証の結果、著作権ラベルを正しく管理するもの(著作権遵守アプリケーションプログラム)であるかが判明し、その認証結果を認証結果記憶部5中に記憶しておく。

【0097】次に、OS3は上記の認証結果記憶部5を調べて、このアプリケーションプログラム6が著作権ラベルを正しく管理するもの(著作権遵守アプリケーションプログラム)であるときにはその要求を認め、そうでないときにはその要求を拒絶する(図12のS66)。これによって、著作物管理を正しく行うことができる。

【0098】本変形例では、アプリケーションプログラムの起動時に認証が行われないために起動速度が向上するほか、著作物を読み書きしないアプリケーションプログラムについては認証処理が全く行われないために上記

第一の実施の形態に比べて実行速度が向上するというメリットがある。

【0099】(変形例9) この変形例9は、上述した第一の実施の形態を、本発明者による特願平6-221235に開示されたデータ入出力管理装置と組合せることにより、著作物データの入出力を管理するようにしたものである。

【0100】この場合のシステム構成を図13に示す。図13において、著作権カーネル4と認証結果記憶部5は上述した第一の実施の形態におけるものと同様の機能を有するものであり、これらを含んだデータ入出力管理装置100が著作物データの読み書き(入出力)を要求する入出力要求プログラム111に対して提供されている。図13のシステムにおけるデータ入出力管理装置100は更に入出力要求受理部101、データ入力部102、保護データ判定部103、保護データ入力記憶部104、出力許諾判定部105、データ出力部106を含む。このデータ入出力管理装置100全体はプロセッサ上のOSで実現できる。

【0101】図13のシステムにおいて、入出力要求プログラム111からの著作物データの読み書き(入出力)要求は、著作権カーネル4と認証結果記憶部5の動作により上述した第一の実施の形態同様このプログラムが著作権ラベルを正しく管理するもの(著作権遵守アプリケーションプログラム)であるとき許可されるほか、著作権遵守アプリケーションプログラムでないプログラムについても著作物データが複製される恐れのない場合には著作物のデータの入出力を認めるようにデータの入出力管理が行われる。

【0102】このようにしても、著作権遵守アプリケーションプログラムでないプログラムが著作物データをコピーすることは出来ないで、著作権侵害を防止するという目的を達成することができる。

【0103】ここで、図13のシステムにおける著作物データの入出力要求に対する動作を簡単に説明するが、詳細は特願平6-221235にあるので省略する。

【0104】まず入出力要求プログラム111が要求を発生すると、入出力要求受理部101がこの要求を受理し、入出力要求プログラム111の識別子と要求の種類を判別する。

【0105】これにより入力要求であることが分ると、データ入力部102が要求されているデータを記憶媒体やネットワーク等から入力する。この時、保護データ判別部103が入力を要求されたデータが保護データ(出力について所定の保護が与えられることを要求されているデータで著作物データを含むもの)であるか否かを判別する。この判別の結果、保護データを含むものであった場合は、保護データ入力記録部104にこの保護データの入力を要求したプログラムの識別子を記録する。そして、入出力要求プログラム111に要求されたデータ

10

20

30

40

50

を与える。

【0106】一方、出力要求であった場合には、著作権遵守アプリケーションプログラムかどうかで処理が異なる。著作権カーネル4に問い合わせを行うことによって認証結果記憶部5を調べ、著作権遵守アプリケーションプログラムであると分った場合には出力を許可する。一方、そうでない場合には、以下の処理を行う。

【0107】出力許諾判定部105が保護データ入力記録部104を調べてこの出力要求を発したプログラムの識別子が記録されているかどうか、即ち、このプログラムが保護データを読んだものであるかどうか、を判定する。ここでこのプログラムの識別子が保護データ入力記録部104に記録されていないければ、このプログラムは保護データを持っていないことになり、このプログラムからの出力要求により保護データが出力される可能性はないので、この場合には出力要求を許諾する。

【0108】これに対し、このプログラムの識別子が保護データ入力記録部104に記録されていれば、このプログラムは保護データを持っていることになり、このプログラムからの出力要求により保護データが出力される可能性がある。従って、この場合には、要求されている出力先に応じて出力要求を認めるかどうか出力許諾判定部105が判断する。ここで、要求されている出力先がディスプレイのように他のプログラムがそこから直接データを読み込めない出力機器である場合には出力要求を許諾し、そうでなければ保護データが複製される恐れがあるため出力要求を拒絶する。出力要求が許諾される場合には、データ出力部106から要求されたデータの出力が行われる。

【0109】これにより、保護データを読んだことのないプログラムからは自由にデータの入出力が行え、且つ、保護データを読んだプログラムからの出力は保護データが複製される恐れのない場合のみ許可するようにデータ入出力管理が行える。

【0110】なお、本発明は上述した各実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【0111】尚、当業者に明らかなように、上述した本発明の実施の形態及びその変形例は、一般の汎用コンピュータを適当にプログラムすることでも実現可能である。この場合に必要となるソフトウェアコードは上述した記載から当業者レベルのプログラマーによって容易に作成可能である。

【0112】特に、上記実施の形態における著作権カーネル4と認証結果記憶部5の機能をソフトウェアパッケージとして実装すると効果的である。

【0113】そのようなソフトウェアパッケージは、上述したような本発明の機能、動作をコンピュータに実現させるようにプログラムするためのコンピュータコードを格納する記憶媒体を用いたコンピュータプログラム製

品の形で提供可能であり、この際の記憶媒体としては、従来のフロッピーディスク、オプティカルディスク、CD-ROM、磁気光学ディスク、ROM、RAM、EPROM、EEPROM、磁気又は光学カード等を含む電子的な命令の格納に適したあらゆる種類の記憶媒体を使用し得るものである。

【0114】

【発明の効果】以上説明したように本発明によれば、アプリケーションプログラムを認証し、その結果を記録するとともに、あるアプリケーションプログラムから著作物データへのアクセス要求があった場合、該アプリケーションプログラムが認証済であるときに限り該アクセス要求を許可するようにしたので、著作権ラベルの管理を正しく行なうものとして登録されたアプリケーションプログラムのみが著作物を操作でき、それ以外のアプリケーションプログラムからの著作物の操作を禁止できるため、著作権の侵害の危険なしに計算機システム上で絵画・小説などの受動的なデータである著作物を処理することができる。

【0115】さらに、本発明では、著作権遵守アプリケーションプログラムを実行させるプロセッサと、認証や認証結果を格納させるプロセッサとを、互いに異なるものとすることによって、認証や著作権データ管理など著作物管理に関わらない前者のプロセッサに係わる部分の管理だけを利用者が行なえるようにし、極めて高いセキュリティを実現できる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態の全体の構成を示すブロック図。

【図2】図1の構成における動作を示すフローチャート。

【図3】図1の構成における動作を説明するための図。

【図4】図1の構成においてアプリケーションプログラムの認証を行なう部分の構成を示す図。

【図5】図1の構成における認証結果記憶部の内部構造を示す図。

【図6】変形例1においてアプリケーションプログラムの認証を行なう部分の構成を示す図。

【図7】変形例2においてアプリケーションプログラムの認証を行なう部分の構成を示す図。

【図8】変形例3の構成を示すブロック図。

【図9】変形例4においてOSの認証を行なう部分の構成を示す図。

【図10】変形例5において著作権ラベルの読み書きを行なう部分の構成を示す図。

【図11】変形例7における認証結果記憶部の内部構造を示す図。

【図12】変形例8における動作を示すフローチャート。

【図13】変形例9の構成を示すブロック図。

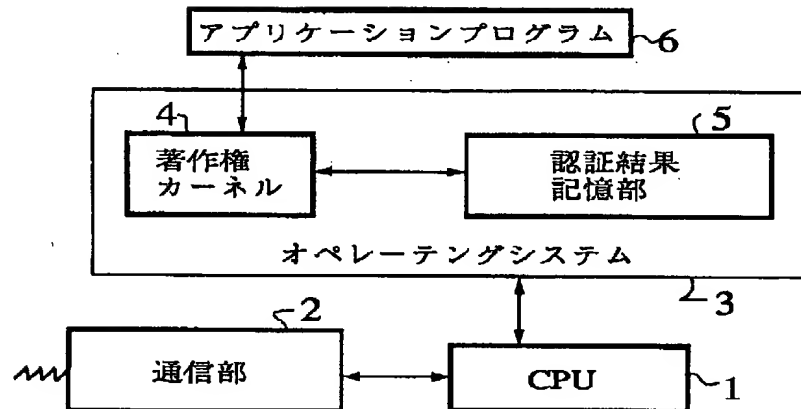
【符号の説明】

- 1 マイクロプロセッサ (CPU)
 2 通信部
 3 オペレーティングシステム (OS)

- * 4 著作権カーネル
 5 認証結果記憶部
 6 アプリケーションプログラム

*

【図1】



【図2】 Fig. 2

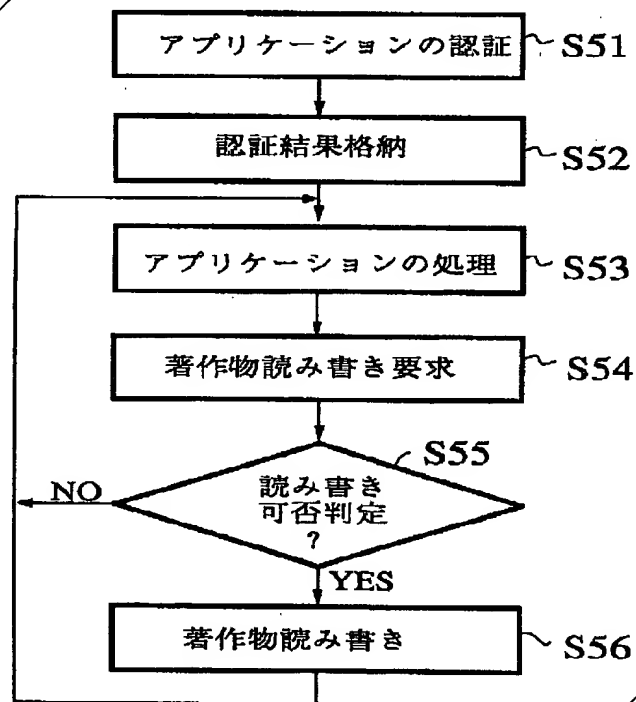
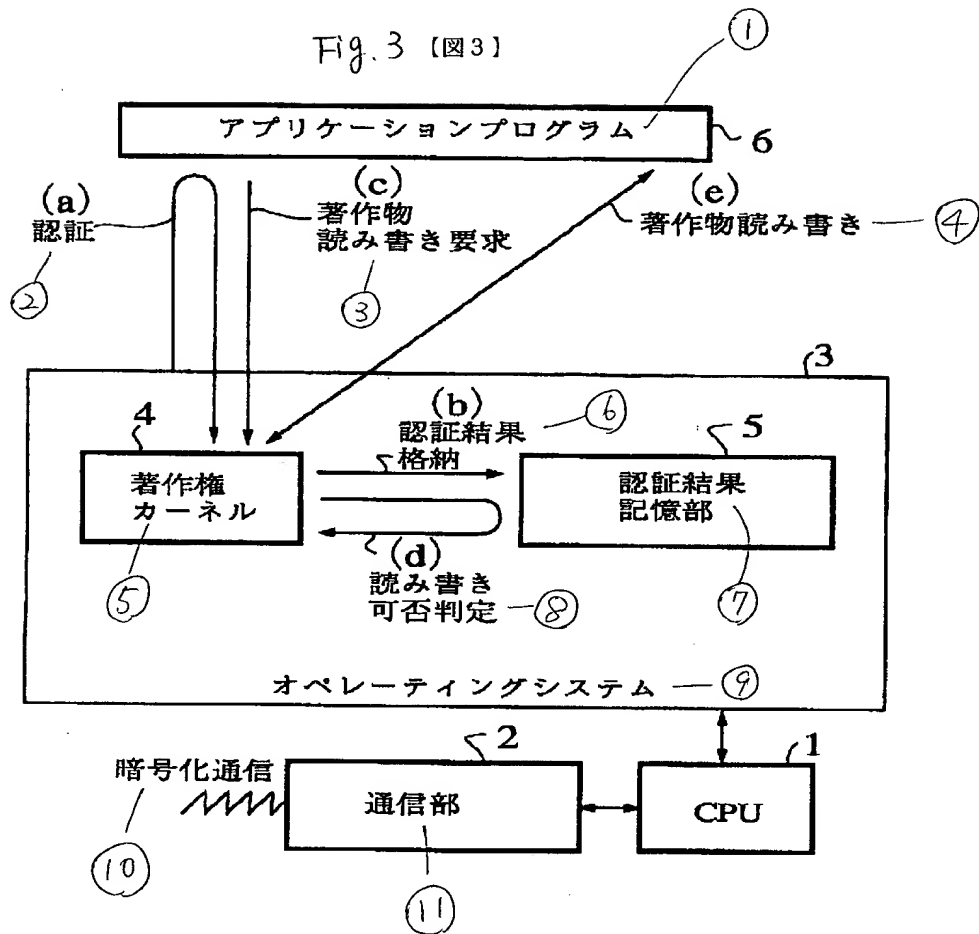
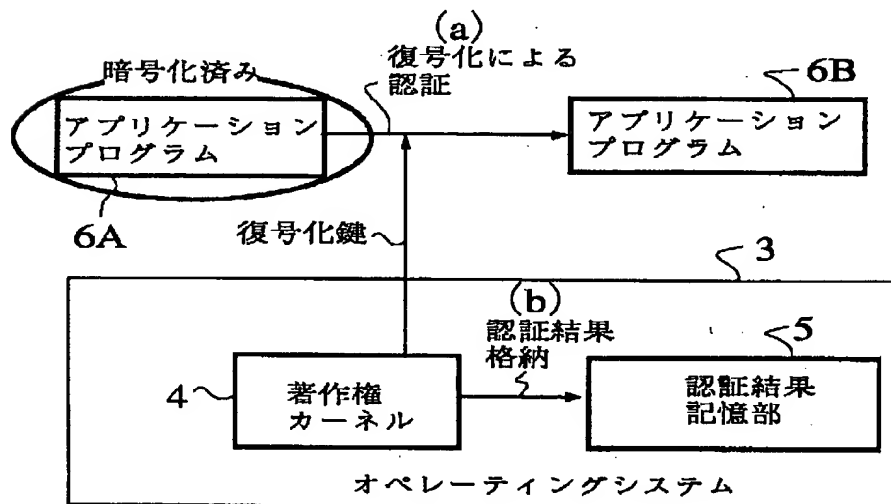


Fig. 3 (図3)



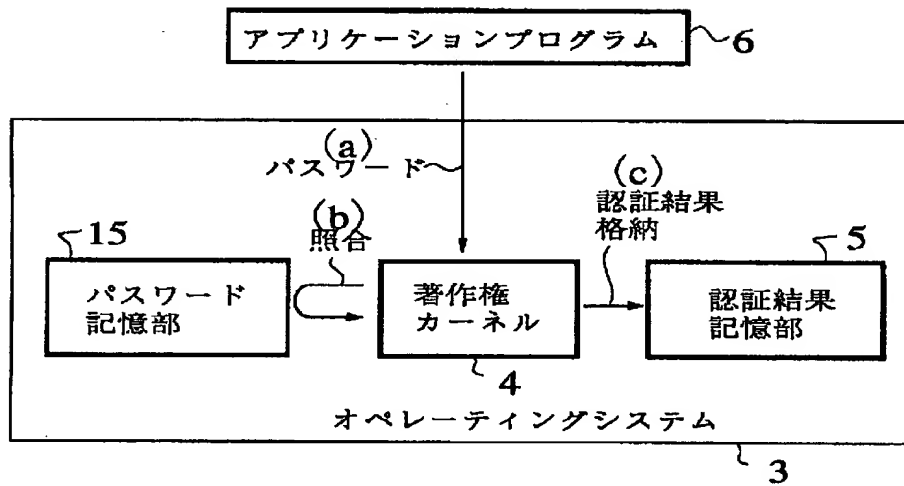
〔図4〕



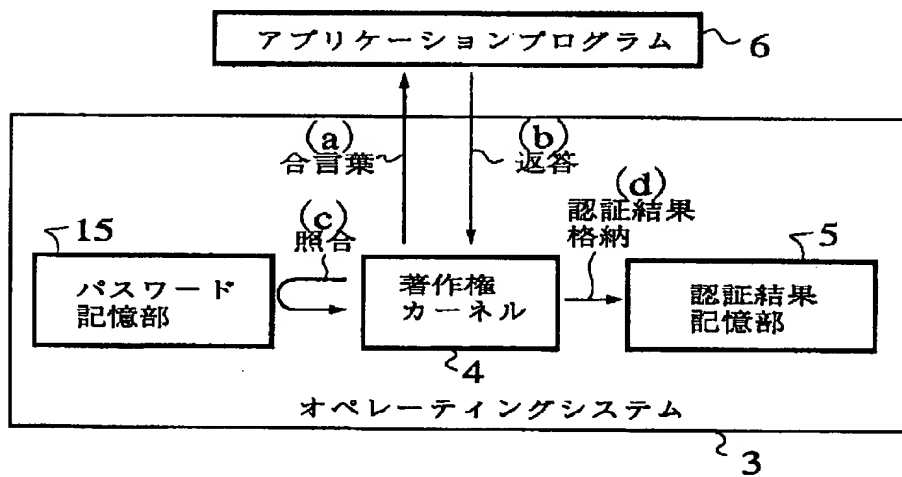
【図5】

	認証結果
アプリケーション プログラム 1	○
アプリケーション プログラム 2	×
.....
アプリケーション プログラム n	○

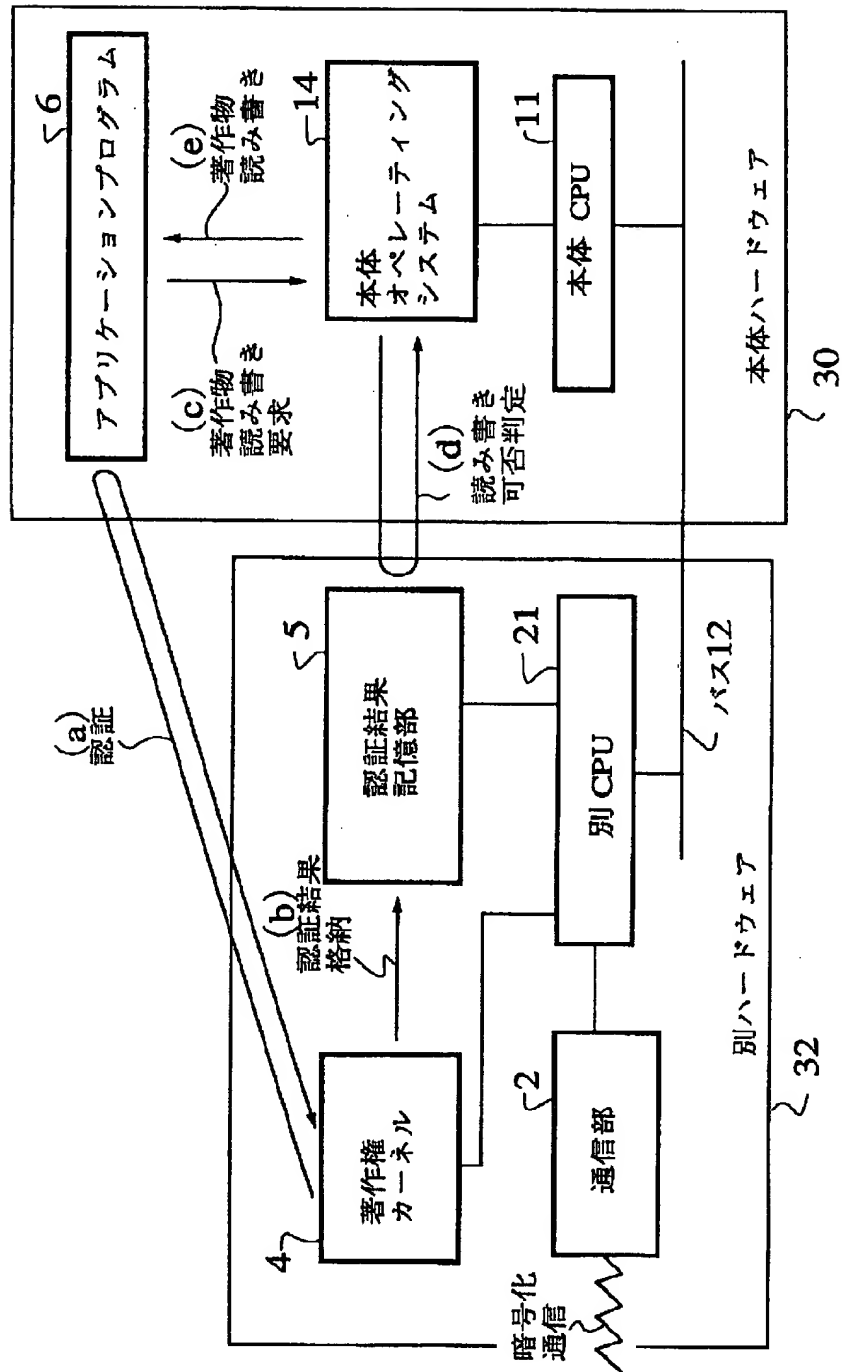
【図6】



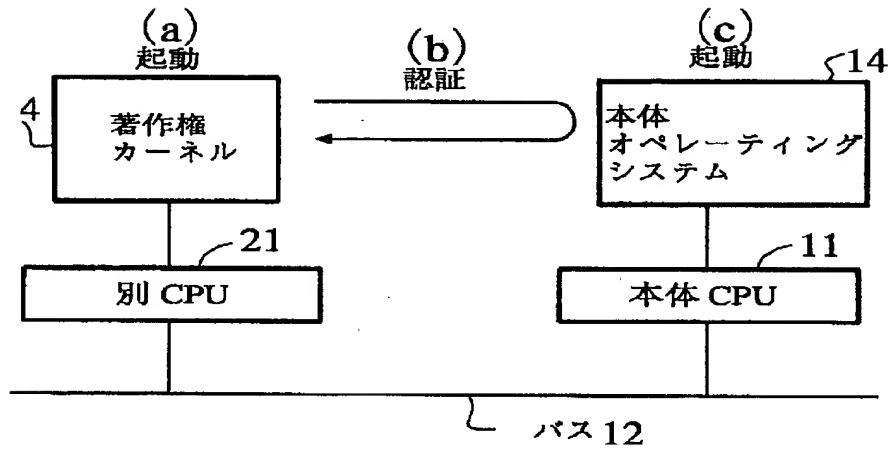
【図7】



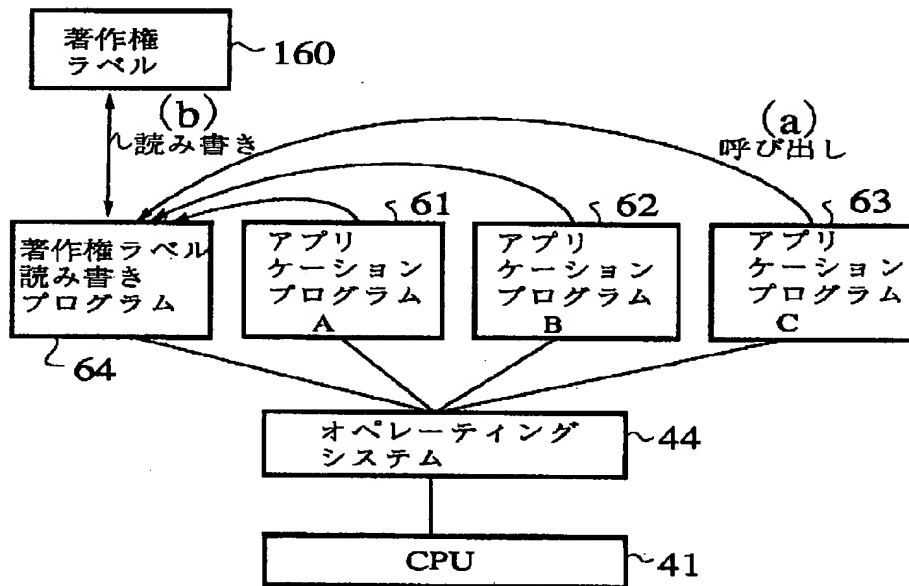
【図 8】



【図 9】



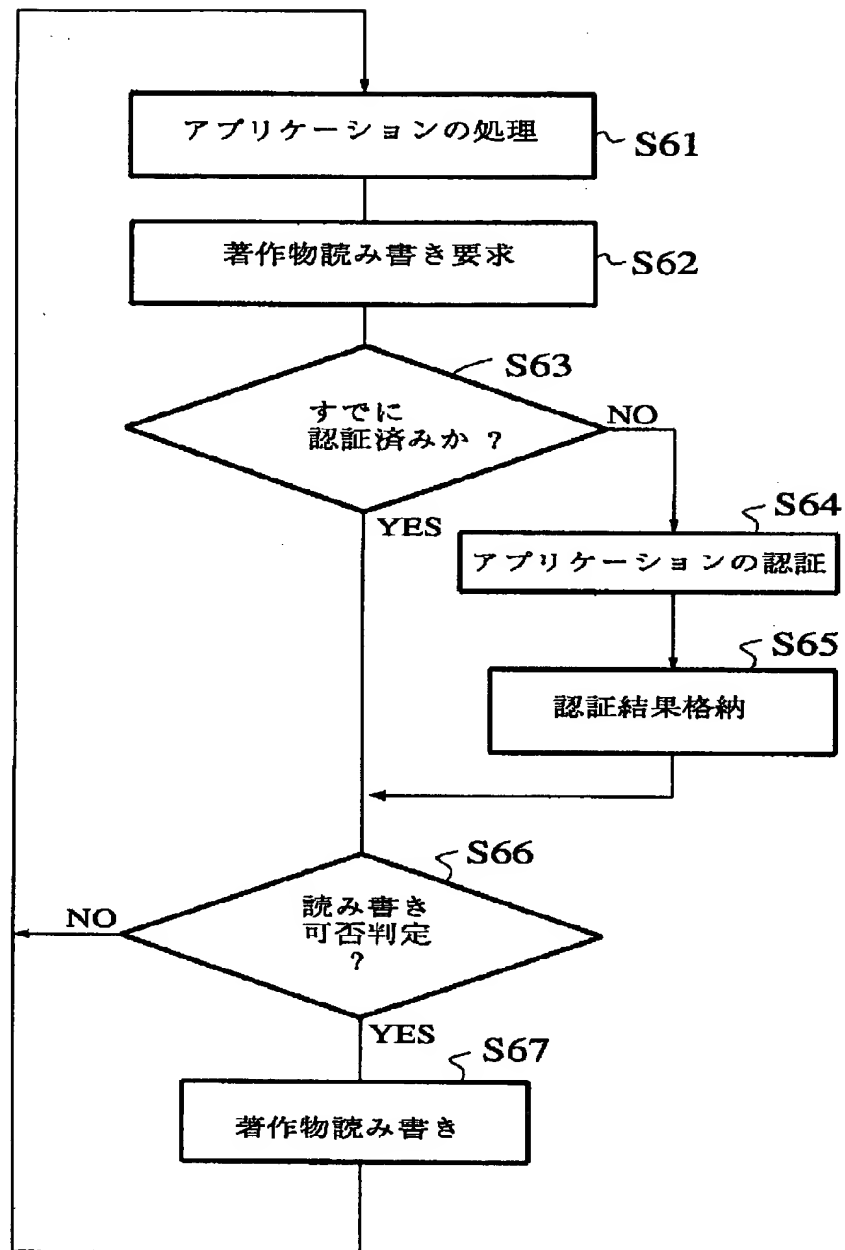
【図 10】



【図 11】

	著作物 1	著作物 2	著作物 n
アプリケーションプログラム 1	○	○	×
アプリケーションプログラム 2	×	○	○
.....
アプリケーションプログラム n	○	×	×

【図12】



【図 13】

